**Product Questions: 131**

**Version: 8.0**

## Question: 1

Which of the following Statements about macros is true? (select all that apply)

1. Arguments are defined at execution time.
2. Arguments are defined when the macro is created.
3. Argument values are used to resolve the search string at execution time.
4. Argument values are used to resolve the search string when the macro is created.

## Answer: A, C

**Question: 2**

What is required for a macro to accept three arguments?

1. The macro's name ends with (3).
2. The macro's name starts with (3).
3. The macro's argument count setting is 3 or more.
4. Nothing, all macros can accept any number of arguments.

## Answer: A

**Question: 3**

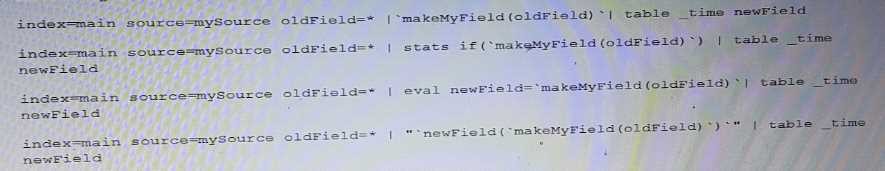
Which of the following statements describes POST workflow actions?

1. POST workflow actions are always encrypted.
2. POST workflow actions cannot use field values in their URI.
3. POST workflow actions cannot be created on custom sourcetypes.
4. POST workflow actions can open a web page in either the same window or a new .

## Answer: D

**Question: 4**

Which of the following searches show a valid use of macro? (Select all that apply)



A. Index=main source=mySource oldField=\* | ‘makeMyField(oldField)’ | table \_time newField

B. Index=main source=mySource oldField=\* | state if(‘makeMyField(oldField)’) | table \_time newField

C. Index=main source=mySource oldField=\* | eval newField=’makeMyField(oldField)’ | table \_time

newField

D. Index=main source=mySource oldField=\* | “’newField(‘makeMyField(oldField)’)’” | table \_time newField

1. Option A
2. Option B
3. Option C
4. Option D

## Answer: A, C

**Question: 5**

Which of the following workflow actions can be executed from search results? (select all that apply)

1. GET
2. POST
3. LOOKUP
4. Search

## Answer: A, B, D

**Question: 6**

Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

1. | datamodel web search | filed web \*
2. | Search datamodel web web | filed web\*
3. | datamodel web web field | search web\*
4. Datamodel=web | search web | filed web\*

## Answer: A

**Question: 7**

Which of the following searches will return events contains a tag name Privileged?

1. Tag= Priv
2. Tag= Priv\*
3. Tag= Priv\*
4. Tag= Privileged

## Answer: D

**Question: 8**

Which of the following statements describes this search?

sourcetype=access\_combined I transaction JSESSIONID | timechart avg (duration)

1. This is a valid search and will display a timechart of the average duration, of each transaction event.
2. This is a valid search and will display a stats table showing the maximum pause among transactions.
3. No results will be returned because the transaction command must include the startswith and endswith options.
4. No results will be returned because the transaction command must be the last command used in the search pipeline.

## Answer: A

**Question: 9**

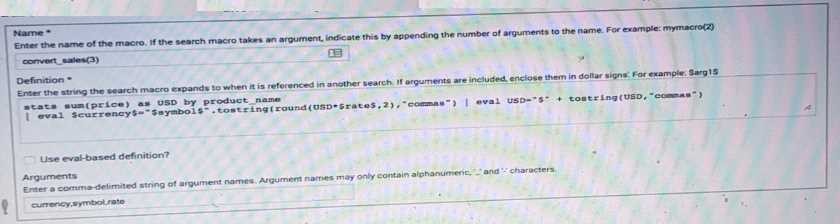
Calculated fields can be based on which of the following?

1. Tags
2. Extracted fields
3. Output fields for a lookup
4. Fields generated from a search string

## Answer: B

**Question: 10**

Based on the macro definition shown below, what is the correct way to execute the macro in search string?



1. Convert\_sales (euro, €, 79)”
2. Convert\_sales (euro, €, .79)
3. Convert\_sales ($euro,$€$,s79$
4. Convert\_sales ($euro, $€$,S,79$)

## Answer: B

**Question: 11**

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

1. Rank
2. Weight
3. Priority
4. Precedence

## Answer: C

**Question: 12**

Which of the following statements describes the command below (select all that apply) sourcetype-access\_combined | transaction JSESSIONID

1. An additional filed named maxspan is created.
2. An additional field named duration is created.
3. An additional field named eventcount is created.
4. Events with the same JSESSIONID will be grouped together into a single event.

## Answer: B, C, D

**Question: 13**

Which of the following can be used with the eval command tostring function (select all that apply)

1. ‘’hex’’
2. ‘’commas’’
3. ‘’Decimal’’
4. ‘’duration’’

## Answer: A, B, D

**Question: 14**

Which of the following statements about tags is true?

1. Tags are case insensitive.
2. Tags are created at index time.
3. Tags can make your data more understandable.
4. Tags are searched by using the syntax tag: : <fieldneme>

## Answer: C

**Question: 15**

Which of the following statements about data models and pivot are true? (select all that apply)

1. They are both knowledge objects.
2. Data models are created out of datasets called pivots.
3. Pivot requires users to input SPL searches on data models.
4. Pivot allows the creation of data visualizations that present different aspects of a data model.

## Answer: D

**Question: 16**

When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

1. Tabs
2. Pipes
3. Colons
4. Spaces

## Answer: A, B, C, D

**Question: 17**

Which of the following describes the Splunk Common Information Model (CIM) add-on?

1. The CIM add-on uses machine learning to normalize data.
2. The CIM add-on contains dashboards that show how to map data.
3. The CIM add-on contains data models to help you normalize data.
4. The CIM add-on is automatically installed in a Splunk environment.

## Answer: C

**Question: 18**

What does the transaction command do?

1. Groups a set of transactions based on time.
2. Creates a single event from a group of events.
3. Separates two events based on one or more values.
4. Returns the number of credit card transactions found in the event logs.

## Answer: B

**Question: 19**

Which of the following statements describe data model acceleration? (select all that apply)

1. Root events cannot be accelerated.
2. Accelerated data models cannot be edited.
3. Private data models cannot be accelerated.
4. You must have administrative permissions or the accelerate\_dacamodel capability to accelerate a data model.

## Answer: B, C

**Question: 20**

A user wants to convert field values to string and also to sort on those value. Which command should be used first, the eval or the sort?

1. It doesn't matter whether eval or sort is used first.
2. Convert the numeric to a string with eval first, then sort.
3. Use sort first, then convert the numeric to a string with eval.
4. You cannot use the sort command and the eval command on the same field.

## Answer: B

**Question: 21**

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

1. Fast mode is enabled.
2. The dashboard is private.
3. The extraction is private.
4. The person in the organization running the report does not have access to the index.

## Answer: C, D

**Question: 22**

Which of the following data model are included In the Splunk Common Information Model (CIM) add-

on? (select all that apply)

1. Alerts
2. Email
3. Database
4. User permissions

## Answer: A, B, C

**Question: 23**

A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

1. Both will appear in the All Fields list, but only if the alias is specified in the search.
2. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.
3. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.
4. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

## Answer: B

**Question: 24**

When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

1. The regex can no longer be edited.
2. The field being extracted will be required for all future events.
3. The events without the required field will not display in searches.
4. Only events with the required string will be included in the extraction.

## Answer: D

**Question: 25**

Which group of users would most likely use pivots?

1. Users
2. Architects
3. Administrators
4. Knowledge Managers

## Question: 26

When using timechart, how many fields can be listed after a by clause?

1. 0 because timechart doesn't support using a by clause.
2. 1 because \_time is already implied as the x-axis.
3. 2 because one field would represent the x-axis and the other would represent the y-axis.
4. There is no limit specific to timechart.

## Answer: B

**Question: 27**

What is the correct syntax to search for a tag associated with a value on a specific fiedsd?

1. Tag-<field?
2. Tag<filed(tagname.)
3. Tag=<filed>::<tagname>
4. Tag::<filed>=<tagname>

## Answer: D

**Question: 28**

What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

1. Macros.
2. Field aliases.
3. The rename command.
4. CIM does not work with different names for the same field.

## Answer: B

**Question: 29**

When should you use the transaction command instead of the stats command?

1. When you need to group on multiple values.
2. When duration is irrelevant in search results. .
3. When you have over 1000 events in a transaction.
4. When you need to group based on start and end constraints.

## Answer: D

**Question: 30**

Which of the following statements describes field aliases?

1. Field alias names replace the original field name.
2. Field aliases can be used in lookup file definitions.
3. Field aliases only normalize data across sources and sourcetypes.
4. Field alias names are not case sensitive when used as part of a search.

## Answer: B

**Question: 31**

What does the following search do?

index=condlog type=mysterymeat action=eaten I stats count as corndogs count by user:

1. Creates a table of the total count of users and split by corndogs.
2. Creates a table of the total count of mysterymeat corndogs split by user.
3. Creates a table with the count of all types of corndogs eaten split by user.
4. Creates a table that groups the total number of users by vegetarian corndogs.

## Answer: B

**Question: 32**

Which of the following statements describes Search workflow actions?

1. By default. Search workflow actions will run as a real-time search.
2. Search workflow actions can be configured as scheduled searches,
3. The user can define the time range of the search when created the workflow action.
4. Search workflow actions cannot be configured with a search string that includes the transaction command

## Answer: C

**Question: 33**

What do events in a transaction have In common?

1. All events In a transaction must have the same timestamp.
2. All events in a transaction must have the same sourcetype.
3. All events in a transaction must have the exact same set of fields.
4. All events in a transaction must be related by one or more fields.

## Answer: B

**Question: 34**

Which of the following statements describe GET workflow actions?

1. GET workflow actions must be configured with POST arguments.
2. Configuration of GET workflow actions includes choosing a sourcetype.
3. Label names for GET workflow actions must include a field name surrounded by dollar signs.
4. GET workflow actions can be configured to open the URI link in the current window or in a new window

## Answer: D

**Question: 35**

Data model are composed of one or more of which of the fo-owing datasets? (select all that apply.)

1. Events datasets
2. Search datasets
3. Transaction datasets
4. Any child of event, transaction, and search datasets

## Answer: A, B, C

**Question: 36**

Which are valid ways to create an event type? (select all that apply)

1. By using the searchtypes command in the search bar.
2. By editing the event\_type stanza in the props.conf file.
3. By going to the Settings menu and clicking Event Types > New.
4. By selecting an event in search results and clicking Event Actions > Build Event Type.

## Answer: C, D

**Question: 37**

Which of the following statements describe the search string below? dacamodel Application\_State All\_Application\_State search

1. Events will be returned from dataset named Application\_state.
2. Events will be returned from the data model named Application\_State.
3. Events will be returned from the data model named All\_Application\_State.
4. No events will be returned because the pipe should occur after the datamodel command

## Answer: B

**Question: 38**

What is the relationship between data models and pivots?

1. Data models provide the datasets for pivots.
2. Pivots and data models have no relationship.
3. Pivots and data models are the same thing.
4. Pivots provide the datasets for data models.

## Answer: D

**Question: 39**

What are the two parts of a root event dataset?

1. Fields and variables.
2. Fields and attributes.
3. Constraints and fields.
4. Constraints and lookups.

## Answer: C

**Question: 40**

In which of the following scenarios is an event type more effective than a saved search?

1. When a search should always include the same time range.
2. When a search needs to be added to other users' dashboards.
3. When the search string needs to be used in future searches.
4. When formatting needs to be included with the search string.

## Answer: D

**Question: 41**

How does a user display a chart in stack mode?

1. By using the stack command.
2. By turning on the Use Trellis Layout option.
3. By changing Stack Mode in the Format menu.
4. You cannot display a chart in stack mode, only a timechart.

## Answer: C

**Question: 42**

Which of the following statements about event types is true? (select all that apply)

1. Event types can be tagged.
2. Event types must include a time range,
3. Event types categorize events based on a search.
4. Event types can be a useful method for capturing and sharing knowledge.

## Answer: B, C

**Question: 43**

In what order arc the following knowledge objects/configurations applied?

1. Field Aliases, Field Extractions, Lookups
2. Field Extractions, Field Aliases, Lookups
3. Field Extractions, Lookups, Field Aliases
4. Lookups, Field Aliases, Field Extractions

## Answer: C

**Question: 44**

Which of the following knowledge objects represents the output of an eval expression?

1. Eval fields
2. Calculated fields
3. Field extractions
4. Calculated lookups

## Answer: B

**Question: 45**

A calculated field maybe based on which of the following?

1. Lookup tables
2. Extracted fields
3. Regular expressions
4. Fields generated within a search string

## Answer: B

**Question: 46**

Which of the following eval command function is valid?

1. Int ()
2. Count ( )
3. Print ()
4. Tostring ()

## Answer: D

**Question: 47**

Which one of the following statements about the search command is true?

1. It does not allow the use of wildcards.
2. It treats field values in a case-sensitive manner.
3. It can only be used at the beginning of the search pipeline.
4. It behaves exactly like search strings before the first pipe.

## Answer: C

**Question: 48**

What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)

1. Custom visualizations
2. Pre-configured data models
3. Fields and event category tags
4. Automatic data model acceleration

## Answer: BC

**Question: 49**

Which of the following file formats can be extracted using a delimiter field extraction?

1. CSV
2. PDF
3. XML
4. JSON

## Answer: A

**Question: 50**

Which of the following statements describes macros?

1. A macro is a reusable search string that must contain the full search.
2. A macro is a reusable search string that must have a fixed time range.
3. A macro Is a reusable search string that may have a flexible time range.
4. A macro Is a reusable search string that must contain only a portion of the search.

## Answer: C

**Question: 51**

Which of the following statements describe calculated fields? (select all that apply)

1. Calculated fields can be used in the search bar.
2. Calculated fields can be based on an extracted field.
3. Calculated fields can only be applied to host and sourcetype.
4. Calculated fields are shortcuts for performing calculations using the eval command.

## Answer: B D

**Question: 52**

Which delimiters can the Field Extractor (FX) detect? (select all that apply)

1. Tabs
2. Pipes
3. Spaces
4. Commas

## Answer: ABCD

**Question: 53**

Which of the following statements is true, especially in large environments?

1. Use the stats command when you next to group events by two or more fields.
2. The stats command is faster and more efficient than the transaction command
3. The transaction command is faster and more efficient than the stats command.
4. Use the transaction command when you want to see the results of a calculation.

## Answer: B

**Question: 54**

Which of the following are required to create a POST workflow action?

1. Label, URI, search string.
2. XMI attributes, URI, name.
3. Label, URI, post arguments.
4. URI, search string, time range picker.

## Answer: C

**Question: 55**

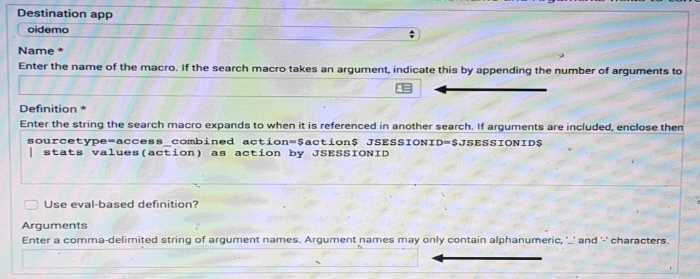
Which of the following statements describe the search below? (select all that apply) Index=main I transaction clientip host maxspan=30s maxpause=5s

1. Events in the transaction occurred within 5 seconds.
2. It groups events that share the same clientip and host.
3. The first and last events are no more than 5 seconds apart.
4. The first and last events are no more than 30 seconds apart.

## Answer: BD

**Question: 56**

Given the macro definition below, what should be entered into the Name and Arguments fileds to correctly configured the macro?



1. The macro name is sessiontracker and the argument are action, JESSION.
2. The macro name is sessiontracker (2) and the action JESSIONID
3. The macro name is sessiontracker and the argument are sectional ,$ JESSIONIDS.
4. The macro name is sessiontracker (2) and the argument are $action ,$JESSIONIDS.

## Answer: B

**Question: 57**

After manually editing; a regular expression (regex), which of the following statements is true?

1. Changes made manually can be reverted in the Field Extractor (FX) UI.
2. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
3. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
4. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

## Answer: D

**Question: 58**

What does the fillnull command replace null values with, it the value argument is not specified?

1. 0
2. N/A
3. NaN
4. NULL

## Answer: A

**Question: 59**

To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

1. Index=main | REJECT trans sessionid
2. Index=main | transaction sessionid | search REJECT
3. Index=main | transaction sessionid | where transaction=reject
4. Index=main | transaction sessionid | where transaction=”REJECT\*”

## Answer: B

**Question: 60**

Which of the following actions can the eval command perform?

1. Remove fields from results.
2. Create or replace an existing field.
3. Group transactions by one or more fields.
4. Save SPL commands to be reused in other searches.

## Answer: B

**Question: 61**

Which of the following statements describe the Common Information Model (CIM)? (select all that apply)

1. CIM is a methodology for normalizing data.
2. CIM can correlate data from different sources.
3. The Knowledge Manager uses the CIM to create knowledge objects.
4. CIM is app that can coexist with other apps on a single Splunk deployment.

## Answer: ABD

**Question: 62**

Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

1. Auto-Extracted fields can be hidden in Pivot.
2. Auto-Extracted fields can have their data type changed.
3. Auto-Extracted fields can be given a friendly name for use in Pivot.
4. Auto-Extracted fields can be added if they already exist in the dataset with constraints.

## Answer: ABCD

**Question: 63**

When creating a Search workflow action, which field is required?

1. Search string
2. Data model name
3. Permission setting
4. An eval statement

## Answer: A

**Question: 64**

Selected fields are displayed each event in the search results.

1. below
2. interesting fields
3. other fields
4. above

## Answer: A

**Question: 65**

A space is an implied in a search string.

1. OR
2. AND
3. ()
4. NOT

## Answer: B

**Question: 66**

Which of the following search control will not re-rerun the search? (Select all that apply.)

1. zoom out
2. selecting a bar on the timeline
3. deselect
4. selecting a range of bars on the timelines

## Answer: BCD

**Question: 67**

Highlighted search terms indicate search results in Splunk.

1. Display as selected fields.
2. Sorted
3. Charted based on time
4. Matching

## Answer: D

**Question: 68**

When you mouse over and click to add a search term this (these) Boolean operator(s) is(are) not implied. (Select all that apply).

A.OR

B.( ) C.AND D.NOT

## Answer: AB

**Question: 69**

The time range specified for a historical search defines the . questionable on ans

A. Amount of data shown on the timeline as data streams in

B. Amount of data fetched from index matching that time range

C. Time range for the static results

## Answer: B

**Question: 70**

Using the export function, you can export search results as . ( Select all that apply)

A.xml

B.json

C.html

D.a php file

## Answer: A, B

**Question: 71**

The fields sidebar does not show . (Select all that apply.)

1. interesting fields
2. selected fields
3. all extracted fields

## Answer: C

**Question: 72**

Splunk alerts can be based on search that run .(Select all that apply.)

1. in real-time
2. on a regular schedule
3. and have no matching events

## Answer: A, B

**Question: 73**

Alert throttling is used to .

1. verify each alert
2. stagger search request in a time sequenced order
3. stop spamming yourself with alerts
4. check severity

## Answer: C

**Question: 74**

A real-time alert is .

1. A scheduled alert
2. constantly running in the background

## Answer: B

**Question: 75**

This tab shows you the event patterns in the results of a specific search.

1. statistics
2. visualization
3. patterns

## Answer: C

**Question: 76**

Which of the following about reports is/are true?

1. Reports are knowledge objects.
2. Reports can be scheduled.
3. Reports can run a script.
4. All of the above.

## Answer: D

**Question: 77**

Select this in the fields sidebar to automatically pipe you search results to the rare command

1. events with this field
2. rare values
3. top values by time
4. top values

## Answer: B

**Question: 78**

A report scheduled to run every 15 mins. but takes 17 mins. to complete is in danger of being .

1. skipped or deferred
2. automatically accelerated
3. deleted
4. all of the above

## Answer: A

**Question: 79**

Which of the following are valid options to speed up reports? (Select all the apply.)

1. Edit permissions
2. Edit description
3. Edit acceleration
4. Edit schedule

## Answer: C

**Question: 80**

Which of the following statements are true for this search? (Select all that apply.) SEARCH: sourcetype=access\* |fields action productld status

1. is looking for all events that include the search terms: fields AND action AND productld AND status
2. users the table command to improve performance
3. limits the fields are extracted
4. returns a table with 3 columns

## Answer: BC

**Question: 81**

Use the dedup command to .

1. Rename a field in the index
2. remove duplicate values
3. rovide an additional alias for the field that can D.be used in the search criteria

## Answer: B

**Question: 82**

We can use the rename command to . (Select all that apply.)

1. Change indexed fields
2. Exclude fields from our search results
3. Extract new fields from our data using regular expressions
4. Give a field a new name at search time

## Answer: D

**Question: 83**

The limit attribute will .

1. override default of 10
2. only work with top command
3. override default of 20
4. override default of 15

## Answer: A

**Question: 84**

This function of the stats command allows you to identify the number of values a field has.

1. max
2. distinct\_count
3. fields
4. count

## Answer: D

**Question: 85**

This function of the stats command allows you to return the sample standard deviation of a field.

1. stdev
2. dev
3. count deviation
4. by standarddev

## Answer: A

**Question: 86**

Which of the following commands will show the maximum bytes?

1. sourcetype=access\_\* | maximum totals by bytes
2. sourcetype=access\_\* | avg (bytes)
3. sourcetype=access\_\* | stats max(bytes)
4. sourcetype=access\_\* | max(bytes)

## Answer: C

**Question: 87**

Which of the following searches will show the number of categoryld used by each host? A.Sourcetype=access\_\* |sum bytes by host

B.Sourcetype=access\_\* |stats sum(categoryld) by host C.Sourcetype=access\_\* |sum(bytes) by host D.Sourcetype=access\_\* |stats sum by host

## Answer: B

**Question: 88**

This clause is used to group the output of a stats command by a specific name

A.rex

B.as

C.list

D.by

## Answer: D

**Question: 89**

This function of the stats command allows you to return the middle-most value of field X.

1. Median(X)
2. Eval by X
3. Fields(X)
4. Values(X)

## Answer: A

**Question: 90**

When a search returns , you can view the results as a list.

1. a list of events
2. transactions
3. statistical values

## Answer: C

**Question: 91**

Clicking a SEGMENT on a chart, .

1. drills down for that value
2. highlights the field value across the chart
3. adds the highlighted value to the search criteria

## Answer: C

**Question: 92**

Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

1. inputlookup
2. lookup

## Answer: B

**Question: 93**

It is mandatory for the lookup file to have this for an automatic lookup to work.

A.Source type

B.At least five columns C.Timestamp

D.Input filed

## Answer: D

**Question: 94**

These users can create global knowledge objects. (Select all that apply.)

1. users
2. power users
3. administrators

## Answer: BC

**Question: 95**

This is what Splunk uses to categorize the data that is being indexed.

1. sourcetype
2. index
3. source
4. host

## Answer: A

**Question: 96**

This is what Splunk uses to categorize the data that is being indexed.

1. Host
2. Sourcetype
3. Index
4. Source

## Answer: B

**Question: 97**

By default search results are not returned in order.

1. Chronological
2. Reverser chronological
3. ASCII
4. Alphabetical

## Answer: AD

**Question: 98**

The stats command will create a by default.

1. Table
2. Report
3. Pie chart

## Answer: A

**Question: 99**

Which is not a comparison operator in Splunk

A. <=

B. =

1. !=
2. >
3. ?=

## Answer: E

**Question: 100**

Which of the following is NOT a stats function:

1. sum
2. addtotals
3. count
4. avg

## Answer: B

**Question: 101**

If a search returns it can be viewed as a chart.

1. timestamps
2. statistics
3. events
4. keywords

## Answer: B

**Question: 102**

In this search, will appear on the y-axis. SEARCH: sourcetype=access\_combined status!=200

| chart count over host

1. status
2. host
3. count

## Answer: C

**Question: 103**

The timechart command buckets data in time intervals depending on:

1. the number of events returned
2. the selected time range
3. the type of visualization selected

## Answer: B

**Question: 104**

Which of these search strings is NOT valid:

1. index=web status=50\* | chart count over host, status
2. index=web status=50\* | chart count over host by status
3. index=web status=5-\* | chart count by host, status

## Answer: A

**Question: 105**

Which command is used to create choropleth choropleth maps?

1. geostats
2. cluster
3. geom

## Answer: C

**Question: 106**

which of the following are valid options with the chart command

1. useother
2. usenull
3. fillfield
4. usefiled

## Answer: AB

**Question: 107**

The gauge command:

1. creates a single-value visualization
2. allows you to set colored ranges for a single-value visualization
3. creates a radial gauge visualization

## Answer: B

**Question: 108**

What will you learn from the results of the following search? sourcetype=cisco\_esa | transaction mid, dcid, icid | timechart avg(duration)

1. The average time elapsed during each transaction for all transactions
2. The average time for each event within each transaction
3. The average time between each transaction

## Answer: A

**Question: 109**

Which of these is NOT a field that is automatically created with the transaction command?

1. maxcount
2. duration
3. eventcount

## Answer: A

**Question: 110**

How many ways are there to access the Field Extractor Utility?

1. 3
2. 4
3. 1
4. 5

## Answer: A

**Question: 111**

When extracting fields, we may choose to use our own regular expressions

1. True
2. False

## Answer: A

**Question: 112**

Field aliases are used to data

1. clean
2. transform
3. calculate
4. normalize

## Answer: D

**Question: 113**

What is the correct way to name a macro with two arguments?

1. us\_sales2
2. us\_sales(1,2)
3. us\_sale,2
4. us\_sales(2)

## Answer: D

**Question: 114**

When using a field value variable with a Workflow Action, which punctuation mark will escape the data

1. \*
2. !
3. ^
4. #

## Answer: B

**Question: 115**

datasets can be added to root dataset to narrow down the search

1. parent
2. extracted
3. event
4. child

## Answer: D

**Question: 116**

Which function should you use with the transaction command to set the maximum total time between the earliest and latest events returned?

1. maxpause
2. endswith
3. maxduration
4. maxspan

## Answer: D

**Question: 117**

The eval command 'if' function requires the following three arguments (in order):

1. Boolean expression, result if true, result if false
2. Result if true, result if false, boolean expression
3. Result if false, result if true, boolean expression
4. Boolean expression, result if false, result if true

## Answer: A

**Question: 118**

Which search would limit an "alert" tag to the "host" field?

1. tag=alert
2. host::tag::alert
3. tag==alert
4. tag::host=alert

## Answer: D

**Question: 119**

The transaction command allows you to events across multiple sources

1. duplicate
2. correlate
3. persist
4. tag

## Answer: B

**Question: 120**

which of the following commands are used when creating visualizations(select all that apply.)

1. Geom
2. Choropleth
3. Geostats
4. iplocation

## Answer: ACD

**Question: 121**

For choropleth maps,splunk ships with the following KMZ files (select all that apply)

1. States of the United States
2. States and provinces of the united states and Canada
3. Countries of the European Union
4. Countries of the World

## Answer: AD

**Question: 122**

Complete the search, …. | failure>successes

1. Search
2. Where
3. If
4. Any of the above

## Answer: B

**Question: 123**

These kinds of charts represent a series in a single bar with multiple sections

1. Multi-Series
2. Split-Series
3. Omit nulls
4. Stacked

## Answer: D

**Question: 124**

When using a split series on a chart, the series MUST be displayed using the STACKED option.

1. True
2. False

## Answer: B

**Question: 125**

Which of the following are valid options with the chart command ?(select all that apply)

1. usenull=f
2. useother=f
3. split=t
4. transcation=t

## Answer: AB

**Question: 126**

This role is required to install the CIM Add-on. Select your answer.

1. ADMIN
2. POWER
3. USER

## Answer: A

**Question: 127**

The Splunk CIM Add-on includes data models in a format. Select your answer.

1. MySQL
2. XML
3. JSON

## Answer: C

**Question: 128**

These allow you to categorize events based on search terms. Select your answer.

1. Groups
2. Event Types
3. Macros
4. Tags

## Answer: B

**Question: 129**

In the Field Extractor Utility, this button will display events that do not contain extracted fields. Select your answer.

1. Selected-Fields
2. Non-Matches
3. Non-Extractions
4. Matches

## Answer: B

**Question: 130**

During the validation step of the Field Extractor workflow:

Select your answer.

1. You can remove values that aren't a match for the field you want to define
2. You can validate where the data originated from
3. You cannot modify the field extraction

## Answer: A

**Question: 131**

Which of the following search modes automatically returns all extracted fields in the fields sidebar?

1. Fast
2. Smart
3. Verbose

## Answer: C